

CLAIMS

1. A method for reading-in a password (p) upon a request of a program (E), the method comprising the steps of:
 - receiving a program-specific identifier ($H(E)$) from said program (E);
 - 5 - receiving said password (p);
 - generating from at least said program-specific identifier ($H(E)$) and said received password (p) a program-password-specific identifier ($F(H(E),p)$); and
 - sending said program-password-specific identifier ($F(H(E),p)$) to said program (E), said program-password-specific identifier ($F(H(E),p)$) being
 - 10 processable by said program (E).
2. Method according to claim 1, wherein
 - the program-specific identifier ($H(E)$) has been derived by applying a first cryptographic function (H) to at least part of the code of the program (E), and
 - the program-password-specific identifier ($F(H(E),p)$) is generated by applying
 - 15 a second cryptographic function (F) to the program-specific identifier ($H(E)$) and at least part of the received password (p), said first cryptographic function (H) and/or said second cryptographic function (F) comprising a hash function, preferably a one-way-hash function, such as MD5 or SHA-1.
- 20 3. Method according to claim 1, wherein a password-reading program (26) and the program-specific identifier ($H(E)$) are provided by means of a trusted computing base (TCB), preferably for both the same trusted computing base (TCB).
- 25 4. Method according to claim 3, wherein the password (p) is received at the password-reading program (26), and, while said password-reading program (26) is executed, all I/O devices are locked and other programs are blocked.

5. Method according to claim 3, wherein the fact that the password-reading program (26) is executed based on the trusted computing base (TCB) is indicated via a signal, preferably by illuminating an LED (28), while the password-reading program (26) receives the password (p).
- 5 6. Method according to claim 1, wherein the program-password-specific identifier ($F(H(E),p,s)$) is generated from the program-specific identifier ($H(E)$), the received password (p), and an additional value (s), said additional value (s) characterizing a device (2) where the program-password-specific identifier ($F(H(E),p,s)$) is generated.
- 10 7. Method according to claim 1, wherein the program-password-specific identifier ($F(H(E),p)$) is used as a key to decrypt another program.
8. A computer program comprising program code means for performing the steps of claim 1 when said program is run on a computer.
- 15
9. A computer program product comprising program code means stored on a computer readable medium for performing the method of claim 1 when said program product is run on a computer.

10. A computer device (2) for reading-in a password (p) upon a request of a program (E) comprising:
- input means (14) for inputting said password (p);
 - receiver means (26) for receiving a program-specific identifier ($H(E)$) and said password (p); and
 - a generator-module (22) connected to said receiver means (26) for generating a program-password-specific identifier ($F(H(E),p)$) from at least said inputted password (p) and said program-specific identifier ($H(E)$), said program-password-specific identifier ($F(H(E),p)$) being processable by said program (E).
11. The computer device (2) according to claim 10, whereby the generator-module (22) is a hash-function generator, and the program-specific identifier ($H(E)$) is derivable from the program (E) by use of said generator-module (22).
12. The computer device (2) according to claim 10 further comprising a trusted computing base (TCB) and indicator means (28) connected to this trusted computing base (TCB).
13. The computer device (2) according to claim 12, whereby the indicator means (28) provides a signal that indicates a secure entry mode while a password-reading program (26) provided by said trusted computing base (TCB) is executable.